TWO ALGORITHMS TO FIND A POWER INTEGRAL BASIS

L HOUSSAIN EL FADIL

Abstract. In this paper, we give an algorithm to compute an integral basis and to test the existence of a power integral basis of $\mathcal{O}$, where $\mathcal{O}$ is the integral closure of $R = k[X]$ in L and L is a finite separable extension of $K = k(X)$. We specify the cases that $L = K[\alpha]$ is a pure cubic (resp. quartic) extension of K.

Introduction

Throughout this paper, $R = k[X]$, where k is a field of characteristic p, $K = k(X)$ is the quotient field of R and $\bar{K}$ is an algebraic closure of K. Let $D \in R$ such that the polynomial $T(Y) = Y^n - D \in R[X]$ is irreducible and $\alpha \in \bar{K}$ a root of $T(Y) = Y^n - D$, such that p does note divide n. Denote $L = K[\alpha]$ and $\mathcal{O}$ the integral closure of R in L. In the second section we find an integral basis of $\mathcal{O}$ as a R-module. We characterize the existence of a power integral basis of $\mathcal{O}$ by a diophantine equation. When $\mathcal{O}$ has a power basis as an R-module, we say that $\mathcal{O}$ is monogenic. We finalize the paper by some examples illustrating this algorithm.
We adopt the following notations : For every prime $\mathcal{P} \in R$, let $K(\mathcal{P}) = R/(\mathcal{P})$ and for every ideal I of R , $v_{\mathcal{P}}(I)$ is the $\mathcal{P}$-valuation of I, defined by $I = J\mathcal{P}^{v_{\mathcal{P}}(I)}$, where J and $\mathcal{P}$ are coprime. Let $\mathbb{F}$ be a field; for two polynomials P and Q lie in $\mathbb{F}[X]$, denote by $D(P, Q)$ their greatest common divisor.

1. Preliminaries

Recall that for two free R-submodules M and N of L, with the same rank over R, there is a nonsingular K-linear map f with $f(M) = N$. The principal ideal of R, generated by the determinant of f, depends only on M and N, which will denote by $[M : N]$, i.e., $[M : N] = det(f)R$. If $N \subset M$, then $[M : N]$ is called the index of N in M. Let Λ be an R-order of L, i.e., Λ is a unitary sub-ring of L, finitely generated as an R-module, which contains a K-basis of L. Since Λ is a finitely generated R-module, $\Lambda \subset \mathcal{O}$. Let $\mathcal{P} \in R$ be a prime; we say that Λ is a $\mathcal{P}$-maximal order of L if $\mathcal{P}$ does

not divide $[\mathcal{O} : \Lambda]$. Λ is a maximal order of L if Λ is a $\mathcal{P}$-maximal order of L for every prime $\mathcal{P}$, i.e., for every prime $\mathcal{P}$, $\mathcal{P}$ does not divide $[\mathcal{O} : \Lambda]$. Let $(u_1, ..., u_n) \in L^n$; denote $D(u_1, ..., u_n)$ the discriminant of $(u_1, ..., u_n)$, i.e., the determinant of the matrix $(T(u_i u_j))_{i,j}$, where T is the trace map of the K-extension L. Let $(e_1, ..., e_n)$ be an R-basis of $\mathcal{O}$; it's well known that $D(u_1, ..., u_n) = \lambda^2 D(e_1, ..., e_n)$, where λ is the determinant of the matrix (x_{ij}), defined by $u_i = \sum_{j=1}^{n} x_{ij} e_j$ for every i. It follows that if $(u_1, ..., u_n)$ is an R-basis of Λ, then $D(u_1, ..., u_n)R = [\mathcal{O} : \Lambda]^2 D(e_1, ..., e_n)$. In particular, $D(1, \alpha, ..., \alpha^{n-1})R = [\mathcal{O} : R[\alpha]]^2 D(e_1, ..., e_n)$.
The Dedekind criterion consists to enlarge the R-order $R[\alpha]$, successively, for every prime $\mathcal{P}$ such that $\mathcal{P}^2$ divides the discriminant δ of $T(X)$, until we obtain the integral closure of R in L as follows : Let $\mathcal{P} \in R$ be a prime such that $\mathcal{P}^2$ divides δ; in $K(\mathcal{P})[X]$, let $\bar{T}(X) = \prod_{i=1}^{r} \bar{t}_i(X)^{e_i}$ be the factorization of $\bar{T}(X)$, of irreducible polynomials in $K(\mathcal{P})[X]$, where $t_1(X), ..., t_r(X)$ are monic polynomials lying in $R[X]$, $g(X) = \prod_{i=1}^{r} t_i(X)$, $h(X)$ is a monic polynomial of $R[X]$ lifts of $\frac{\bar{T}(X)}{\bar{g}(X)}$ and $f(X) = \frac{gh(X) - T(X)}{\mathcal{P}} \in R[X]$. If $D(\bar{f}, \bar{g}, \bar{h}) = 1$, then $R[\alpha]$ is a $\mathcal{P}$-maximal R-order of $K[\alpha]$. Else, let U be a monic polynomial of $R[X]$ lifts of $\bar{U}(X) = \frac{\bar{T}}{D(\bar{f}, \bar{g}, \bar{h})}$; then $R[\alpha] + \frac{1}{\mathcal{P}} U(\alpha) R[\alpha]$ is an an R-order of $K[\alpha]$, which is very large than $R[\alpha]$ (see [1, 2]).

2. Main results

In this section, we use the Dedekind criterion to find an integral basis of $\mathcal{O}$ and then, we give an algorithm to test if $\mathcal{O}$ has a power integral basis.

Let $T(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in R[X]$ and $\mathcal{P}$ a prime of R. We say that T is of Eisenstein type with respect to the prime $\mathcal{P}$ if $\mathcal{P}$ divides every a_i and $\mathcal{P}^2$ does not divide a_0. The following Lemma generalizes the Lemma 1, page 11 cited in [4].

Lemma 2. 1. *Let $T(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in R[X]$ be an irreducible polynomial, α a root of $T(X)$ and $\mathcal{P}$ a prime of R. If T is of Eisenstein type with respect to the prime $\mathcal{P}$, then $R[\alpha]$ is a $\mathcal{P}$-maximal R order of $K[\alpha]$.*

Proof. In $K(\mathcal{P})[X]$, $g(X) = X$ and $h(X) = X^{n-1}$, and then $f(X) = \frac{\sum_{k=0}^{n-1} a_k X^k}{\mathcal{P}}$. Since $\mathcal{P}^2$ does not divide a_0, $f(0) \neq 0$ modulo $\mathcal{P}$. Therefore, $D(\bar{g}, \bar{h}, \bar{f}) = 1$. Hence $R[\alpha]$ is a $\mathcal{P}$-maximal R order of $K[\alpha]$. ■

Theorem 2. 2. *Let $D \in R$ be a cubic free such that $T = Y^3 - D$ is an irreducible polynomial and $p \neq 3$. Set $D = AB^2$, where A and B are coprime square free in the principal domain R. Then $\mathcal{B} = (1, \alpha, \frac{1}{B}\alpha^2)$ is an integral basis of $\mathcal{O}$.*

Proof. Let $\delta = \bar{+}9D^2$ be the discriminant of $T(Y)$. Use the Dedekind criterion, it suffices to enlarge, successively, $R[\alpha]$ for every prime $\mathcal{P}$ of R which divides D.
If $\mathcal{P}$ divides A, then T is of Eisenstein type with respect to the prime $\mathcal{P}$ and then, $R[\alpha]$ is a $\mathcal{P}$-maximal R order of $K[\alpha]$. Else, i.e., if $\mathcal{P}$ divides B, then $f(0) = 0$ modulo $\mathcal{P}$ and then, $D(\bar{f}, \bar{g}, \bar{h}) = Y$. Therefore, $R[\alpha] + \frac{1}{\mathcal{P}}\alpha^2 R[\alpha]$ is an R-order of $R[\alpha]$, which is very large than $R[\alpha]$. On the other hand, let $X^3 - \frac{D}{\mathcal{P}^3}$ be the minimal polynomial of $\frac{\alpha}{\mathcal{P}}$ and $X^3 - \frac{D^2}{\mathcal{P}^6}$ the minimal polynomial of $\frac{1}{\mathcal{P}^2}\alpha^2$. So, $\frac{1}{\mathcal{P}}\alpha$ and $\frac{1}{\mathcal{P}^2}\alpha^2$ are not integral over R. Let $A(\alpha) = a_0 + a_1\alpha + \frac{a_2}{\mathcal{P}}\alpha^2 \in \mathcal{O}$, such that every $a_i \in K$ and $\mathcal{P}A(\alpha) \in R[\alpha]$. Then $(b_0 = \mathcal{P}a_0, b_1 = \mathcal{P}a_1, a_2) \in R^3$ and $B(\alpha) = a_0 + a_1\alpha = A(\alpha) - a_2\frac{1}{\mathcal{P}}\alpha^2 \in \mathcal{O}$. If $a_1 \neq 0$, consider $X^3 - \frac{3b_0}{\mathcal{P}}X^2 + \frac{3b_0^2}{\mathcal{P}^2}X + \frac{-b_1^3 d - b_0^3}{\mathcal{P}^3}$ the minimal polynomial of $B(\alpha)$. Since $B(\alpha) \in \mathcal{O}$, $\mathcal{P}$ divides b_0 and then, $\mathcal{P}$ divides b_1. Therefore, $A(\alpha) = a_0 + a_1\alpha + b_2\frac{\alpha^2}{\mathcal{P}}$, where $(a_0, a_1, b_2) \in R^3$. Consequently, $R[\alpha] + \frac{\alpha^2}{\mathcal{P}}R[\alpha]$ is a $\mathcal{P}$-maximal order of $K[\alpha]$. Therefore, $[\mathcal{O} : R[\alpha]] = BR$. As $(\frac{1}{B}\alpha^2)^3 = \frac{D^2}{B^3} = A^2B$, $\frac{1}{B}\alpha^2$ is integral over R and then, $\mathcal{B} = (1, \alpha, \frac{1}{B}\alpha^2)$ is an integral basis of $\mathcal{O}$. ■

Theorem 2. 3. *Let $D \in R$ be a quartic free such that $T = Y^4 - D$ is an irreducible polynomial and $p \neq 2$. Let $D = AB^2C^3$, where A, B and C are pairwise-coprime square free in the principal domain R. Then $\mathcal{B} = (1, \alpha, \frac{1}{BC}\alpha^2, \frac{1}{BC^2}\alpha^2)$ is an integral basis of $\mathcal{O}$.*

Proof. Let $\delta = \bar{+}4^4D^3$ be the discriminant of $T(Y)$. Use the Dedekind criterion, it suffices to enlarge, successively, $R[\alpha]$ for every prime $\mathcal{P}$ of R which divides D. Let $\mathcal{P}$ divides D.
1^{st} case $\mathcal{P}$ divides A. Then T is of Eisenstein type with respect to the prime $\mathcal{P}$ and then, $R[\alpha]$ is a $\mathcal{P}$-maximal R order of $K[\alpha]$.
2^d case $\mathcal{P}$ divides B. In $K(\mathcal{P})[Y]$, $g(Y) = Y$, $h(Y) = Y^3$ and $f(Y) = \frac{D}{\mathcal{P}}$. Since $\mathcal{P}^2$ divides D, $f(0) = 0$ modulo $\mathcal{P}$ and then, $D(\bar{f}, \bar{g}, \bar{h}) = Y$. So, $R[\alpha] + \frac{1}{\mathcal{P}}\alpha^3 R[\alpha]$ is an R-order of $R[\alpha]$, which is very large than $R[\alpha]$. On the other hand, since $X^4 - AC^3\frac{B^2}{\mathcal{P}^4}$, $X^2 - AC^3\frac{B^2}{\mathcal{P}^2}$, $X^2 - AC^3\frac{B^2}{\mathcal{P}^4}$, $X^4 - A^3C^9\frac{B^6}{\mathcal{P}^4}$ and $X^4 - A^3C^9\frac{B^6}{\mathcal{P}^8}$ are respectively the minimal polynomials, over K, of $\frac{\alpha}{\mathcal{P}}$, $\frac{1}{\mathcal{P}}\alpha^2$, $\frac{1}{\mathcal{P}^2}\alpha^2$, $\frac{\alpha^3}{\mathcal{P}}$ and $\frac{\alpha^3}{\mathcal{P}^2}$. Then $\frac{1}{\mathcal{P}}\alpha^2$ and $\frac{\alpha^3}{\mathcal{P}}$ are integral over R and $\frac{\alpha}{\mathcal{P}}$, $\frac{1}{\mathcal{P}^2}\alpha^2$ and $\frac{1}{\mathcal{P}^2}\alpha^3$ are not integral over R. Let $A(\alpha) = a_0 + a_1\alpha + a_2\frac{\alpha^2}{\mathcal{P}} + a_3\frac{\alpha^3}{\mathcal{P}} \in \mathcal{O}$, such that every $a_i \in K$ and $\mathcal{P}A(\alpha) \in R[\alpha]$. Then $(b_0 = \mathcal{P}a_0, b_1 = \mathcal{P}a_1, a_2, a_3) \in R^4$ and $B(\alpha) = a_0 + a_1\alpha = A(\alpha) - b_2\frac{1}{\mathcal{P}}\alpha^2 - b_3\frac{1}{\mathcal{P}}\alpha^3 \in \mathcal{O}$. If $a_1 \neq 0$, consider $X^4 - \frac{4b_0}{\mathcal{P}}X^3 + \frac{6b_0^2}{\mathcal{P}^2}X^2 - \frac{4b_0^3}{\mathcal{P}^3}X - \frac{(b_0^4 - b_1^4 d)}{\mathcal{P}^4}$, the minimal polynomial of $B(\alpha)$, then $\mathcal{P}$ divides b_0 and b_1. Therefore, the R-order generated by $(1, \alpha, \frac{1}{\mathcal{P}}\alpha^2, \frac{1}{\mathcal{P}}\alpha^3)$ is a $\mathcal{P}$-maximal R-order of $K[\alpha]$ and then,

$v_{\mathcal{P}}([\mathcal{O}:R[\alpha]])=2$.
3^{th} case $\mathcal{P}$ divides C. Consider $X^4-AB^2\frac{C^3}{\mathcal{P}^4}$, $X^2-AB^2\frac{C^3}{\mathcal{P}^2}$, $X^2-AB^2\frac{C^3}{\mathcal{P}^4}$, $X^4-A^3B^6\frac{C^9}{\mathcal{P}^8}$ and $X^4-A^3B^6\frac{C^9}{\mathcal{P}^{12}}$ respectively, the minimal polynomials over K, of $\frac{\alpha}{\mathcal{P}}$, $\frac{1}{\mathcal{P}}\alpha^2$, $\frac{1}{\mathcal{P}^2}\alpha^2$, $\frac{\alpha^3}{\mathcal{P}^2}$ and $\frac{\alpha^3}{\mathcal{P}^3}$. Then $\frac{1}{\mathcal{P}}\alpha^2$ and $\frac{\alpha^3}{\mathcal{P}^2}$ are integral over R and $\frac{\alpha}{\mathcal{P}}$,$\frac{\alpha^2}{\mathcal{P}^2}$ and $\frac{1}{\mathcal{P}^3}\alpha^3$ are not integral over R. As in the previous case, let $A(\alpha)=a_0+a_1\alpha+a_2\frac{1}{\mathcal{P}}\alpha^2+a_3\frac{1}{\mathcal{P}^2}\alpha^3\in\mathcal{O}$, such that every $a_i\in K$ and $\mathcal{P}^2A(\alpha)\in R[\alpha]$. Then $(b_0=\mathcal{P}^2a_0,b_1=\mathcal{P}^2a_1,b_2=\mathcal{P}a_2,a_3)\in R^4$ and then, $B(\alpha)=a_0+a_1\alpha+a_2\frac{1}{\mathcal{P}}\alpha^2$ is integral over R. Let $X^4-4\frac{b_0}{\mathcal{P}^2}X^3+\frac{(-2b_2^2d+6b_0^2)}{\mathcal{P}^4}X^2+\frac{(-4b_1^2b_2d+4b_2^2db_0-4b_0^3)}{\mathcal{P}^6}X+\frac{(4b_0b_1^2b_2d-2b_2^2db_0^2-b1^4d+b_0^4+b2^4d^2)}{\mathcal{P}^8}$ be the characteristic polynomial of $B(\alpha)$. Consider respectively the coefficients of X^3, X^2 and X, we conclude that $\mathcal{P}^2$ divides b_0, $\mathcal{P}$ divides b_2 and $\mathcal{P}^2$ divides b_1. So, the R-order generated by $(1,\alpha,\frac{1}{\mathcal{P}}\alpha^2,\frac{1}{\mathcal{P}^2}\alpha^3)$ is a $\mathcal{P}$-maximal R-order of $K[\alpha]$ and then, $v_{\mathcal{P}}([\mathcal{O}:R[\alpha]])=3$.
Consequently, $[\mathcal{O}:R[\alpha]]=B^2C^3R$. As $(\frac{1}{BC}\alpha^2)^2=AC$ and $(\frac{1}{BC^2}\alpha^3)^4=A^3B^2C$, $\frac{1}{BC}\alpha^2$ and $\frac{1}{BC^2}\alpha^2$ are integral over R. Finally, $\mathcal{B}=(1,\alpha,\frac{1}{BC}\alpha^2,\frac{1}{BC^2}\alpha^2)$ is an integral basis of $\mathcal{O}$. ■

Now, we give an algorithm to test if $\mathcal{O}$ is monogenic.
For every $(x_0,x_1,..,x_{n-1})\in R^n$, let $\theta=\sum_{i=0}^{n-1}x_i\frac{1}{r_i}\alpha^i$. For every $2\leq i\leq n-1$, let $\theta^i=\sum_{k=0}^{n-1}f_{ik}\frac{1}{r_k}\alpha^k$, where every f_{ik} is a polynomial of $R[x_0,x_1,..,x_{n-1}]$.

Let $\lambda(x_0,x_1,..,x_{n-1})=\begin{vmatrix} x_1 & f_{21}, & ... & f_{n-11} \\ x_2 & f_{22}, & ... & f_{n-12} \\ . & . & ... & . \\ . & . & ... & . \\ . & . & ... & . \\ x_{n-1} & f_{2n-1}, & ... & f_{n-1n-1} \end{vmatrix}$.

Lemma 2. 4. *Under the above hypothesis, $\mathcal{O}$ is monogenic if and only if there exists $(x_0,x_1,..,x_{n-1})\in R^n$ such that $\lambda(x_0,x_1,..,x_{n-1})$ is invertible in R.*

Proof. It's well known that $[\mathcal{O}:R[\theta]]=\lambda R$, where $\lambda=\lambda(x_0,x_1,..,x_{n-1})$. Thus $\mathcal{O}=R[\theta]$ if and only if λ is invertible in R. ■

In the following we give a detail study of the cases that $n\in\{3,4\}$.

Cubic extensions

Let $p\neq 3$, $D\in R$ be a cubic free, i.e., $D=AB^2$, where $D(A,B)=1$ and A and B are square free. Let $\alpha\in\bar{K}$ be a root of the irreducible polynomial $T(X)=Y^3-D$ and $\mathcal{O}$ the integral closure of $L=K[\alpha]$. In this section, our

aim is to give an algorithm to test if $\mathcal{O}$ is monogenic and to find a power integral basis of $\mathcal{O}$.

Theorem 2. 5. *$\mathcal{O}$ is monogenic if and if there exists $(y,z) \in R^2$ such that $By^3 - Az^3$ is invertible in R.*

Proof. From Theorem 2.2, $\mathcal{B} = (1, \alpha, \frac{1}{B}\alpha^2)$ is an integral basis of $\mathcal{O}$. For every $(x,y,z) \in R^3$, let $\theta = x+y\alpha+z\frac{1}{B}\alpha^2$. Then $\theta^2 = (\frac{2xz}{B+y^2})\alpha^2+(z^2A+2xy)\alpha+x^2+2yzAB$. Hence $\lambda(x,y,z) = \begin{vmatrix} y & (z^2A+2xy) \\ z & B(\frac{2xz}{B+y^2}+y^2) \end{vmatrix} = By^3-Az^3$. ■

Remark that : Since $\lambda(x,y,z)$ is independent on the choice of x, we can assume that $x = 0$.

Corollary 2. 6. *Under the hypothesis of this subsection, if $degree(B-A) = 0$ or D is square free or $D = uB^2$, where $u \in k*$, then $\mathcal{O}$ is monogenic.*

Proof. If $B - A$ is invertible, then $\lambda(0,1,1) = B - A$. Hence $\mathcal{O} = R[\theta]$, where $\theta = \alpha + \frac{\alpha^2}{B}$.
If D is square free, i.e., B is invertible. It follows that $\lambda(0,1,0) = B$ and then, $\mathcal{O} = R[\alpha]$.
If $D = uB^2$, i.e., A is invertible, then $\lambda(0,0,1) = -A$. Hence $\mathcal{O} = R[\theta]$, where $\theta = \frac{\alpha^2}{B}$. ■

After this study, we give the following algorithm:
In put : A polynomial D.
Out put : An integral basis of $\mathcal{O}$ and an answer of the question : $\mathcal{O}$ is it monogenic?
1) Factorize D as AB^2P^4 and replace D by AB^2.
2) If $D \notin k[X]^3$, then i) $\mathcal{B} = (1, \alpha, \frac{1}{B}\alpha^2)$ is an integral basis of $\mathcal{O}$.
ii) Solve the equation (E): $By^3 - Az^3$ in $\overline{k(X)}^2$.
3) If (E) has a solution in $k[X]^2$, then $\mathcal{O}$ is monogenic and conclude a power integral basis. Else $\mathcal{O}$ is not monogenic.

Quartic extensions

Theorem 2. 7. *Let $p \neq 2$, $D \in R$ be a quartic free, i.e., $D = AB^2C^3$, where A, B, C are pairwise-coprime square free and $T(X) = Y^4 - D$ is an irreducible polynomial. Let $\alpha \in \bar{K}$ be a root of $T(X) = Y^4 - D$ and $\mathcal{O}$ the integral closure of R in $L = K[\alpha]$. Then $\mathcal{O}$ is monogenic if and if there exists $(y,z,t) \in K[X]^3$ such that $-4z^4t^2A^2C - 8y^3BC^2tAz^2 + 4AC^2z^4y^2 +$*

$8yt^3A^2BCz^2 - t^6A^3B^2 + y^6B^2C^3 - t^4A^2B^2Cy^2 + y^4B^2C^2At^2$ *is invertible in* $K[X]$.

Proof. From Theorem 2.3, $\mathcal{B} = (1, \alpha, \frac{1}{BC}\alpha^2, \frac{1}{BC^2}\alpha^3)$ is an integral basis of $\mathcal{O}$. For every $(x, y, z, t) \in R^4$, let $\theta = x + y\alpha + z\frac{1}{BC}\alpha^2 + t\frac{1}{BC^2}\alpha^2$. Then $f_{02} = x^2 + AC(2ytB + z^2)$, $f_{12} = 2xy + 2ztA$, $f_{22} := 2xz + BCy^2 + t^2AB$, $f_{32} = 2xt + 2yzC$, $f_{13} = (x^2 + AC(2ytB + z^2))y + (2xy + 2ztA)x + A((2xz + y^2BC + t^2AB)t + (2xt + 2yzC)z)$, $f_{23} = ((x^2 + AC(2ytB + z^2))z + (2xy + 2ztA)BCy + (2xz + y^2BC + t^2AB)x) + AB(2xt + 2yzC)t$, And $f_{33} = ((x^2 + AC(2ytB + z^2))t + (2xy + 2ztA)zC + (2xz + y^2BC + t^2AB)Cy + (2xt + 2yzC)x)$. Thus,
$\lambda(x, y, z, t) = -4z^4t^2A^2C - 8y^3BC^2tAz^2 + 4AC^2z^4y^2 + 8yt^3A^2BCz^2 - t^6A^3B^2 + y^6B^2C^3 - t^4A^2B^2Cy^2 + y^4B^2C^2At^2$. ■

Remark that : Since $\lambda(x, y, z, t)$ is independent on the choice of x, we can assume that $x = 0$.

Corollary 2. 8. *If D is square free or D is a cub, then $\mathcal{O}$ is monogenic.*

Indeed, if BC is invertible, then $\lambda(0, 1, 0, 0) = B^2C^3$ is invertible.
If AB is invertible, then $\lambda(0, 1, 0, 0) = -A^3B^2$ is invertible. ■

References

[1] H. Cohen, A course in computational algebraic number theory, GTM 138, Springer-Verlag Berlin Heidelberg, New York, Paris, Tokyo, second correction, 1995.

[2] L. El fadil, Computational of the integral closure. (to appear in International Journal of Commutative Rings)

[3] L. El Fadil and M. Charkani. Generalization of the discriminant and applications, The Arabian Journal for Science and Engineering, (1A)29, 2004, 93-98.

[4] M. Ishida, The genus fields of algebraic number fields, lec. Notes in Maths 555, Springer-Verlag. Berlin. Heidelberg. New York, 1976.

[5] A. Fröhlich and M. Taylor, Algebraic number theory, Combridge Studies in Advenced Mathematics 27,CUP, 1992.

[6] L.C. Washington. Introduction to cyclotomic fields, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

L houssain EL FADIL,
Lycée Reda Slaoui (CPGE),
B.P. 3149, Talborjt, Agadir
Agadir-Morocco